(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 April 2002 (18.04.2002)

PCT

(10) International Publication Number
WO 02/31618 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/SG00/00173

(22) International Filing Date: 13 October 2000 (13.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **KENT RIDGE DIGITAL LABS** [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **XU, Changsheng** [CN/SG]; Block 701, #06-337, West Coast Road, Singapore 120701 (SG). **WU, Jiankang** [CN/SG]; Block 51, #06-565, Teban Gardens Road, 600051 SINGAPORE (SG).

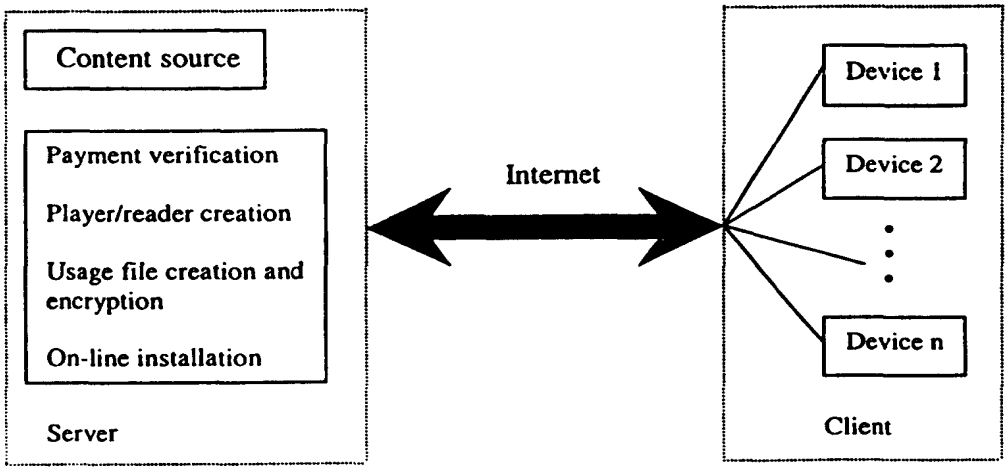
(74) Agent: **HELEN YEO & PARTNERS**; #33-00 UOB Plaza 1, 80 Raffles Place, Singapore 048624 (SG).

(81) Designated States *(national)*: GB, SG, US.

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR CONTROLLING USAGE AND PROTECTING AGAINST COPYING OF DIGITAL MULTIMEDIA CONTENT AND ASSOCIATED PLAYERS/READERS



(57) Abstract: The present invention presents a method and system for controlling usage and protecting against copying of digital multimedia content (such as audio, video, image, and document) and their associated players or readers. The system is arranged so that digital content and their players or readers that are installed in one computer or device cannot be used if they are copied to another computer or device. The system may also be arranged so that duplicated digital content is not usable in the same computer or device. Usage data associated with each item of digital content may restrict the running time during which the content can be used and may be updated automatically after each usage of the content. The content may not be accessible if its permitted usage has expired.

WO 02/31618 A2

METHOD AND SYSTEM FOR CONTROLLING USAGE AND PROTECTING AGAINST COPYING OF DIGITAL MULTIMEDIA CONTENT AND ASSOCIATED PLAYERS/READERS

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to a method and system for controlling usage and protecting against copying of digital multimedia content and their associated players or readers.

Description of Related Art

Rapid development of computer networks and increased use of multimedia data via the Internet have resulted in faster and more convenient exchange of digital information or content. However, the open environment of the Internet creates consequential problems with respect to enforcement of copyright in artistic works, and in particular, illegal distribution of digital multimedia works without the owner's authorization. To dissuade illegal copying, there exists a need for strengthening and assisting enforcement of copyright protection of such works. Typically, security measures and digital watermarking technologies have been used to protect digital content. Firstly, the digital content is stored in a cryptographic container before distribution to users. Secondly, a flexible licensing mechanism is used to control the right of those seeking access to the content. Thirdly, watermarks are embedded in the content in an imperceptible fashion so that the content can be identified if the cryptographic container is breached. Whilst security measures and watermarking technologies are effective in protecting digital content to some extent, distinct problems exist in actual applications. Neither security measures nor digital watermarking can prevent digital content being illegally duplicated and distributed. In order to better protect digital content and its usage, the present invention provides copy protection and usage control for digital multimedia content and their associated players or readers installed in a digital computer or device.

Various methods of copy protection and usage control have been developed to prevent unauthorized use of software. Compared with these methods, the present invention is more effective and simpler.

The prior art technologies fall into two categories. The first category is hardware-based. In this first category is U.S. Pat. No. 4,562,306 which discloses a method for protecting

computer software using an active coded hardware device, which must be plugged into the computer's communication port before the software can be run. U.S. Pat. No. 4,866,769 discloses a copy protection system for PC software distributed on discs, which provides a unique ID stored in a RAM of a PC in which software on a disc is to be used. This ID is accessible to the user of the computer. Prior to each use of the program, the software on the disc uses the PC and the source IDs and checkword to verify that the software is being used on the same PC on which it was installed. U.S. Pat. No. 4,849,836 discloses a system for preventing copying of software from computer disks, the system including a key sequence in a copy protection section of a program which is deliberately rendered ambiguous by repeatedly recording a word containing that sequence while gradually shifting the phase of the transition of a portion of the sequence until the sequence becomes a different sequence. U.S. Pat. No. 5,758,068 discloses a method and apparatus for software license management. It uses three identifier codes from a computer to control the access and usage of the software to this computer. These methods can restrict the use of the software to a single computer system, but they need additional hardware support and are not flexible.

The second category is software-based. In this second category is U.S. Pat. No. 5,199,066 which discloses a method and apparatus for protecting software in which the use of software is enabled only when a predetermined intermediate code and a predetermined software code are identical. U.S. Pat. No. 5,109,413 discloses a method that allows software distributors to control the length of time or the number of times a user can run protected software. This method provides a trial period during which a potential purchaser can decide whether or not he or she wants to buy the software. After the trial period expires, either new software without usage control system is provided or instructions are given to users to disable the usage control system. U.S. Pat. No. 5,293,422 discloses a usage control system for computer software. The software comprises a set of units, each of the units being an interactive activity between the software and the user which can be separately completed from the interactive activities of the other units in the set. The completion of units is monitored by means of a copy-protected region of a recording medium and when all units have been completed, further access to the software is denied. Although these approaches have to some extent limited use of computer software, they cannot provide adequate protection against duplication of the software and are susceptible to being circumvented.

SUMMARY OF THE INVENTION

The present invention provides a method for protecting digital content. The method may prevent digital content and their players or readers from being illegally duplicated and distributed, and may control and update permitted usage rights relating to the digital content.

According to the present invention there is provided a method of protecting digital content to be installed to a client device from a remote server, said method including the steps of: creating a player/reader for said digital content; creating a usage file associated with said digital content, said usage file including storage paths defining locations in said client device for storing copies of said usage file; embedding at least said storage paths in said player/reader to provide a protection enabled player/reader; installing said digital content and said protection enabled player/reader to said client device; installing said copies of said usage files in said locations defined by said storage paths; and adapting said protection enabled player/reader to verify the existence of said copies of said usage files at said locations in said client device prior to each playing/reading of said digital content.

The method of the present invention may control usage of digital content on a personal computer or other device. The term "device" will be used herein to describe a PC (Personal Computer) or other terminal suitable for accessing digital content via the internet. In order to further protect the digital content and prevent its illegal use, encryption and watermarking techniques may be used to code the digital content. Encryption may ensure that the digital content cannot be used without an encryption key. Each item of digital content may be encrypted with a different key. Watermarking, may provide proof of copyright of the digital content and may facilitate tracing of illegal distributions of the digital content in the event that the encryption is breached.

Copy protection according to the present invention may be arranged such that duplicated versions of original digital content cannot be played or read once it is installed in a client computer or device. The installed digital content also may not be copied from one computer or device to another computer or device, nor may it be renamed. A player or reader installed in one computer or device may not be used in another computer or device.

The present invention may rely upon on-line facilities such as the internet to install the digital content purchased by a client. In a transaction process, the client may be required to provide to a server which loads the digital content his personal information and configuration of his computer or device. The server may embed the relevant information into the associated player or reader and send it to the client computer or device. Meanwhile, the item of digital content and its associated files may be installed in relevant locations of the client computer or device according to information embedded into the associated player or reader. If the digital content is to be correctly played or read by the player or reader, all of the associated files will need to exist in the correct locations of the computer or device.

The usage file may include usage data, the encryption key and other information relating to an item of digital content. All usage files downloaded to the same client computer or device may be encrypted using the same key. This key may be embedded into the associated content player or reader. The encrypted usage file may be redundantly installed in different locations of the client computer or device. The locations are dependant on information embedded in the player or reader, obtained from the client and his computer or device. To play or read an item of digital content, all encrypted usage files corresponding to this item of content must exist in the client computer or device. Furthermore, a summary file may be created for each client computer or device. The summary file may contain a name identifying the digital content, details of any encryption key used to encrypt the digital content, and current usage data relating to the digital content installed on a particular computer/device. The summary file may be encrypted using the same key as the usage files and may be stored redundantly in locations of the computer/device identical to the locations of the usage files. The summary file may be updated after each playing or reading of the item of digital content. If permitted usage of an item of digital content has expired, usage files corresponding to this item of content may be deleted from the computer/device. The relevant record in the summary file may also be deleted. Without these files, the expired content cannot be played or read by the player or reader. If the client wants to replay or reread the digital content, he/she must connect to the server and request to install the content and relevant files to his computer/device.

A usage control mechanism may be adopted to enforce terms and conditions of use of the digital content. Business rules may be associated with the digital content to be distributed. The usage control mechanism may be used to specify variable licensing parameters to manage and enforce terms and conditions of use. The usage control mechanism may encompass means for monitoring and tracing use of the digital content for reporting to owners of copyright in digital content. The usage control mechanism may be tamper-resistant and may be integrated into content protection mechanisms.

DESCRIPTION OF THE DRAWINGS

A preferred embodiment of the present invention will be described with reference to the accompanying drawings wherein:

Fig 1 shows the general structure of a communications network between a client and a server;

Fig 2 shows a flow chart of a process associated with an online installation transaction;

Fig 3 shows a block diagram of a process for creating protected content;

Fig 4 shows a block diagram of a process for creating a protection enabled player/reader;

Fig 5 shows a flow chart of a process for installation of digital content in an on-line route:

Fig 6 shows a flow chart of a process for creating and updating a summary file; and

Fig 7 shows a flow chart of a process for playing/reading digital content.

DETAILED DESCRIPTION

Fig.1 illustrates the general structure of communications between a client computer or device 10 (PC or other access devices) and a server 11 providing a source of content & associated services. Server 11 may include one or more sources for storing digital content and databases for current distribution. The services provided by server 11 include payment verification, player/reader creation, usage file creation and encryption, and on-line installation.

Fig.2 illustrates a flow chart of a process associated with an online installation transaction, commencing with the client sending a request (20) to server 11 for digital content to be installed on client device 10. The request includes the content name, conditions of usage and payment, and information about the configuration of client device 10. Assuming that

payment is verified as correct (21,22) and it is the first time that the digital content is being installed on client device 10 (23), a player or reader corresponding to the digital content is created (24) and sent (25) to the client device 10. Meanwhile, a usage file corresponding to the content is created (26) and encrypted. The encrypted usage file together with the encrypted digital content is installed (27) on client device 10 via the on-line installation service incorporated in server 11.

To secure the digital content against unauthorised use and to monitor or trace illegal distribution of the digital content in the event that security is breached, encryption and watermarking is used to generate a secure digital content format. Fig.3 shows a block diagram of an encryption and watermarking process. An imperceptible watermark is embedded in the digital content to provide marked content that may be identified as content that is subject to copyright protection. The watermark may be embedded in the plain or original digital content in any suitable manner and by any suitable means as is known in the art. The watermarked digital content is then encrypted using an encryption key corresponding to the content. The watermarked content may be encrypted in any suitable manner and by any suitable means as is known in the art. The encrypted and watermarked content is stored in the content source associated with Server 11.

When an item of digital content is to be distributed to client device 10, the relevant usage file is created and installed on client device 10 together with the content. The usage file includes the content name, its usage data (number of permitted playing/reading times, expiry date, etc), together with its encryption key. Each item of digital content to be distributed may correspond to a usage file. All usage files on the same device may be encrypted using an identical key. This key may be embedded into the players or readers for that device.

If the digital content being installed in client device 10 for the first time, the player/reader used to play/read the digital content is also installed on this device. The encryption key used to encrypt the usage files, the paths used to store the usage files in clients device 10, and a usage check and updating module may be embedded into a traditional player/reader to produce a protection enabled player/reader. The protection enabled player/reader of

present invention is different from a traditional player/reader in that it can not only play/read the secure content, but is also able to distinguish original content and duplicated content as well as check usage of the digital content. If the content is duplicated or the permitted usage of the content has expired, the player/reader will be disabled and will not be able to play/read the content. Fig.4 illustrates the block diagram of the creation of a protection enabled player/reader.

In order to ensure that duplicated content cannot be played/read by the player/reader and to control usage of digital content, the digital content and its usage file should be installed on a client's device via an on-line route.

Fig.5 illustrates the flowchart of an on-line installation process. Before the client can install an item of digital content on his device 10, he/she needs to answer some questions so that server 11 can obtain information about the configuration of the client device 10. Assuming that the client device 10 is installing the digital content for the first time (50), installation paths for the content and its usage files are created(51). The paths are embedded into the content player/reader (52) and stored together with device information (53) into the database at server 11.

The player/reader is then sent via the internet to client device 10 (54). If client device 10 has already installed the player/reader, the digital content and its usage files will be installed on this device according to the installation paths and device information embedded in the player/reader (55). After installation, a content file and multiple redundant usage files are installed on client device 10. Redundant usage files are installed in different locations defined by the installation paths to facilitate copy protection. A client who installs an item of digital content and its usage files on his/her device, may know the location of the content, but will not know the locations of the usage files.

Before an item of digital content can be played/read, it may not be sufficient to produce the content and its usage files. A summary file for each device may also be required and information associated with the content may be included in the summary file. The summary file may be created by the player/reader when the digital content is first

played/read on a device. The information and usage data associated with all items of digital content installed in this device may be included in the summary file. The usage data associated with an item of content in the summary file may be updated after each playing/reading of the item. The summary file may include a name identifying the content, its encryption key, and its usage data. Fig.6 illustrates a flowchart of a summary file creation and updating process.

The present invention may provide copy protection and usage control. Copy protection may deny duplicated versions of original digital content the capacity to be played/read on another device. Copy protection may also deny the original content the capacity to be played/read on the device if eg., a permitted time frame for the item of content has expired, and may deny a renamed version of the original content the capacity to be played/read on the original or another device. Usage control may provide for playing/reading of content to comply with terms & conditions of usage as determined at the time of purchase. Usage control may ensure that any item of content cannot be played/read if its permitted usage time has expired.

Fig.7 illustrates the flowchart of how an item of digital content can be correctly played/read. According to Fig.7 two conditions must be satisfied to play an item of content. Firstly, the usage files corresponding to the item of content must exist in correct locations in the associated device as indicated by paths embedded into the player/reader. Secondly, the summary file must include the information and usage data associated with the item of content. These two conditions may ensure that duplicated versions of the content cannot be played/read beyond its permitted usage either on the same device or on another devices. The locations in which the usage files and the summary file are stored will be different for different devices. These locations are recorded in the players/readers distributed to the respective devices. The client will only know the location where the digital content are stored, but will not know where the usage files and summary file are stored.

Each item of content is encrypted with a unique key and these keys are recorded in the usage file and summary file. The usage file and summary file are encrypted using an identical key and this key is embedded in the player/reader.

If a client makes copies of the digital content and the player/reader attempts to play the copied version of the content on another device, the content will not be played/read because the relevant usage files and summary file do not exist on that device. If the client plays the copied version of the content on the original device, the summary file will be updated in the same manner as if the client had played/read the original content. If the client renames the copied file, it cannot be played/read because there will be no match with corresponding usage files. If usage of an item of digital content has expired, the player/reader may delete the relevant usage files associated with this item of content and may also delete elements associated with these content included in the summary file. Even if the item of content can be reserved after its usage has expired, it cannot be played/read because its usage files have been deleted from the device.

It is to be understood that various alterations, modifications and/or additions may be introduced into the construction and arrangement of the parts herein described without departing from the spirit or ambit of this invention.

CLAIMS:

1. A method of protecting digital content to be installed to a client device from a remote server, said method including the steps of:

creating a player/reader for said digital content;

creating a usage file associated with said digital content, said usage file including storage paths defining locations in said client device for storing copies of said usage file;

embedding at least said storage paths in said player/reader to provide a protection enabled player/reader;

installing said digital content and said protection enabled player/reader to said client device;

installing said copies of said usage files in said locations defined by said storage paths;

and adapting said protection enabled player/reader to verify the existence of said copies of said usage files at said locations in said client device prior to each playing/reading of said digital content.

2. A method according to claim 1 including the step of disabling said protection enabled player/reader if said protection enabled player/reader is unable to detect said copies of said usage files at said locations defined by the storage paths embedded therein.

3. A method according to claim 1 including the step of embedding a digital watermark into said digital content.

4. A method according to claim 3 including the step of encrypting the watermarked digital content by means of a watermark encryption key.

5. A method according to claim 4 wherein said watermark encryption key is unique to each item of digital content.

6. A method according to claim 1 including the step of encrypting said usage file by means of a usage encryption key.

7. A method according to claim 6 including the step of embedding said usage encryption key into said protection enabled player/reader.

8. A method according to claim 6 wherein said usage encryption key is identical for each usage file installed to said client device.

9. A method according to claim 1 wherein said client device includes a personal computer.

10. A method according to claim 1 wherein said usage file includes usage data associated with said digital content and details relating to any encryption key used to encrypt said digital content.

11. A method according to claim 1 including the step of embedding a summary file creation and updating module into said protection enabled player/reader.

12. A method according to claim 11 wherein said module is adapted to create a summary file prior to a first playing/reading of said digital content on said client device.

13. A method according to claim 12 wherein said module is adapted to update said summary file after each playing/reading of said digital content on said client device.

14. A method according to claim 12 wherein said summary file includes a name identifying said digital content, details of any encryption key used to encrypt the digital content and current usage data.

15. A method according to claim 13 wherein said digital content includes any copy of said digital content.

16. A method according to claim 14 wherein said summary file includes usage expiry information relating to an item of digital content and including the step of disabling said protection enabled player/reader if said current usage data indicates that permitted usage of said item of digital content has expired.

17. A method according to claim 16 wherein said usage expiry information includes a permitted usage expiry date or number of permitted playing/reading times.

18. A method according to claim 16 wherein said step of disabling includes the step of deleting one or more usage files associated with said item of digital content.

19. A method according to claim 1 wherein said client device is connectable to said remote server via a network such as the internet.

20. A method according to claim 1 wherein said digital content includes multimedia such as digital audio, video, image and document.

21. A system for implementing a method according to any one of the preceding claims.

DRAWINGS

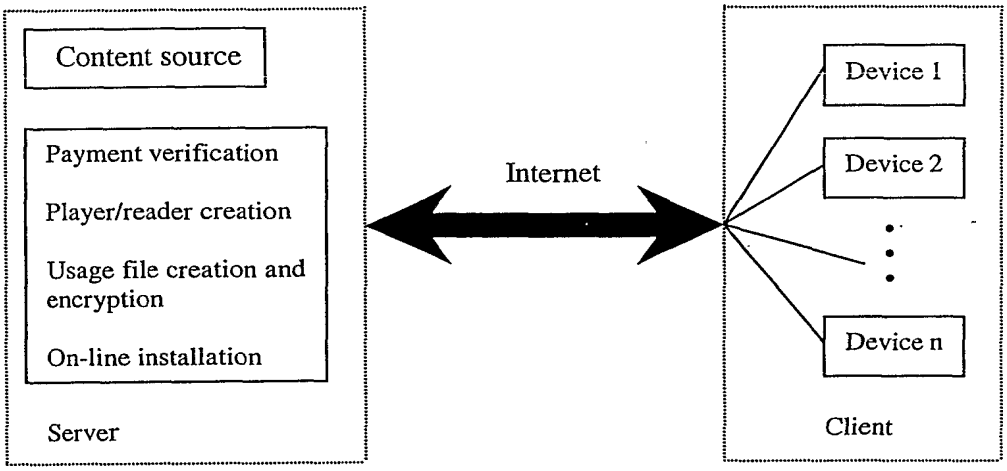


Fig.1

11 10

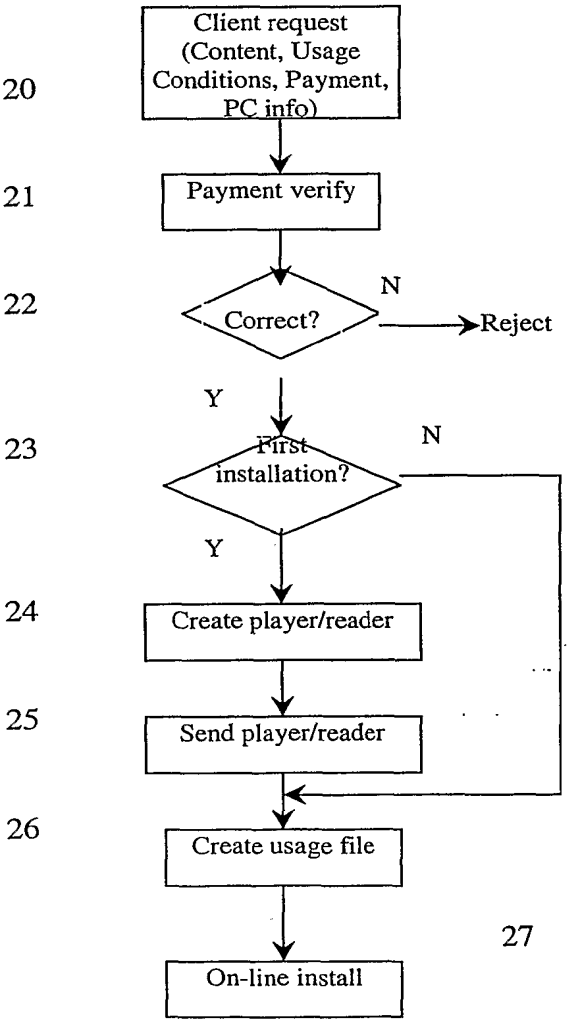


Fig.2

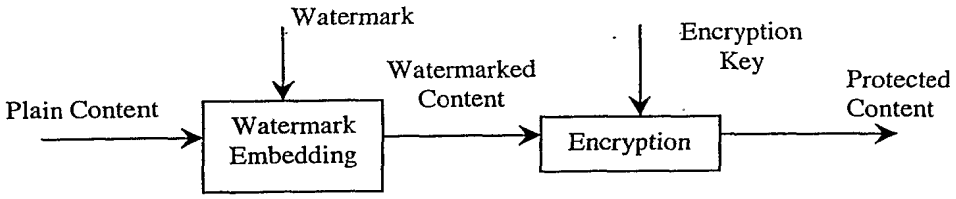

Watermark
Encryption Key
Watermarked Content
Protected Content
Plain Content
Watermark Embedding
Encryption

Fig.3

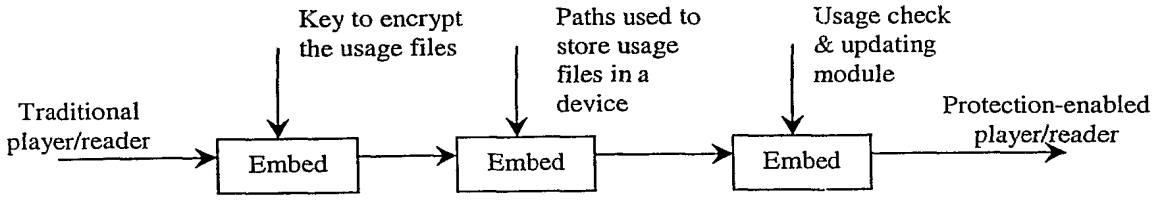

Key to encrypt the usage files
Paths used to store usage files in a device
Usage check & updating module
Traditional player/reader
Protection-enabled player/reader
Embed
Embed
Embed

Fig.4

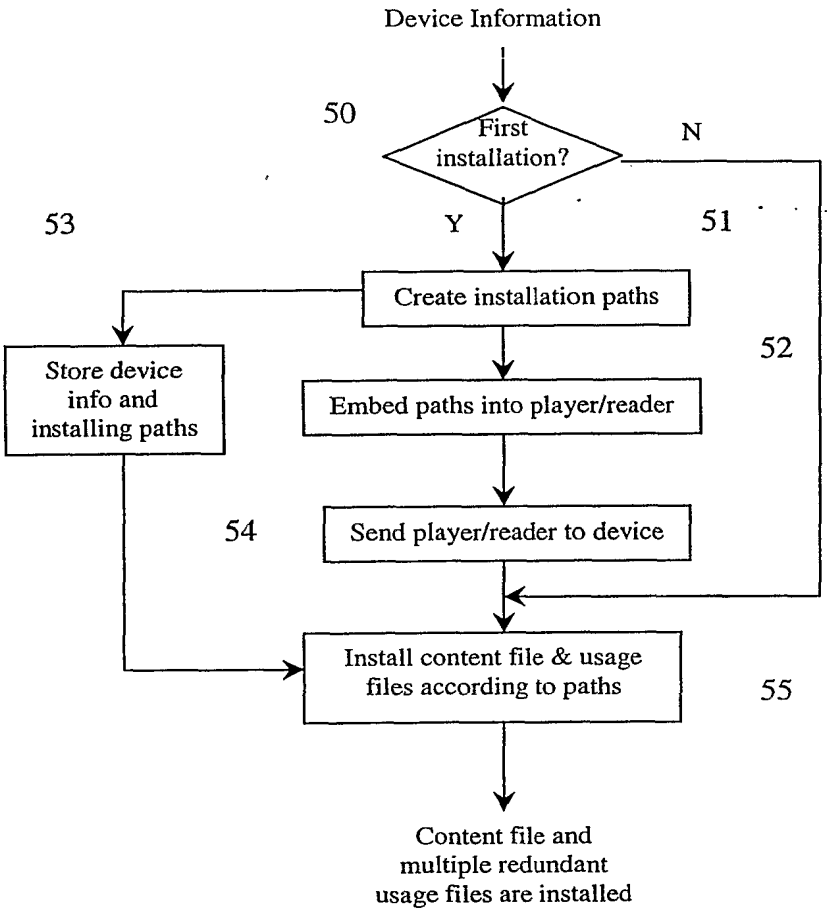

Device Information
50
First installation?
N
53
Y
51
Create installation paths
52
Store device info and installing paths
Embed paths into player/reader
54
Send player/reader to device
Install content file & usage files according to paths
55
Content file and multiple redundant usage files are installed

Fig.5

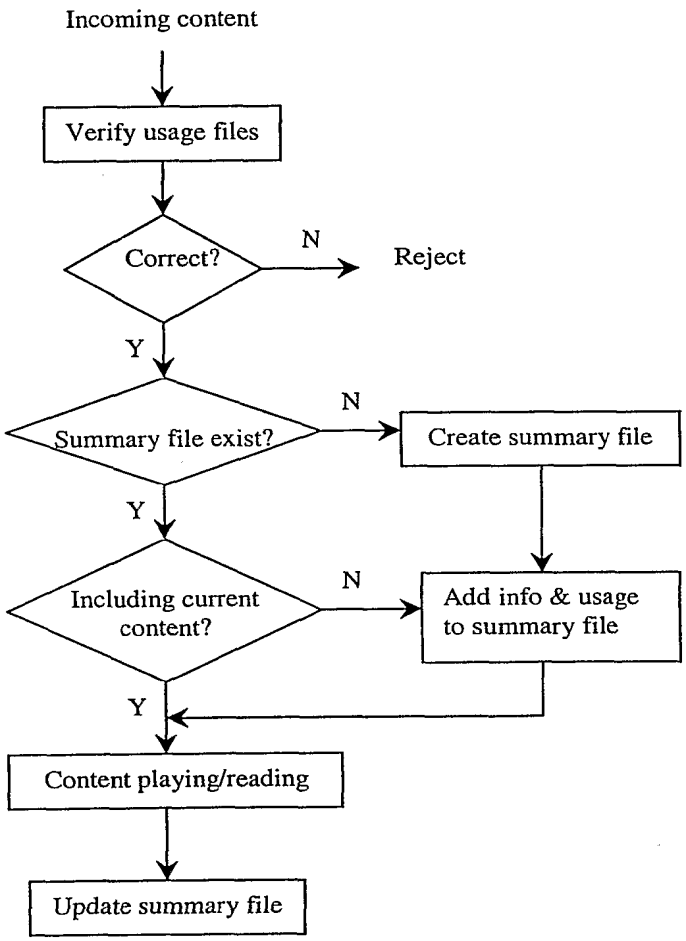

Incoming content
Verify usage files
Correct?
N
Reject
Y
Summary file exist?
N
Create summary file
Y
Including current content?
N
Add info & usage to summary file
Y
Content playing/reading
Update summary file

Fig.6

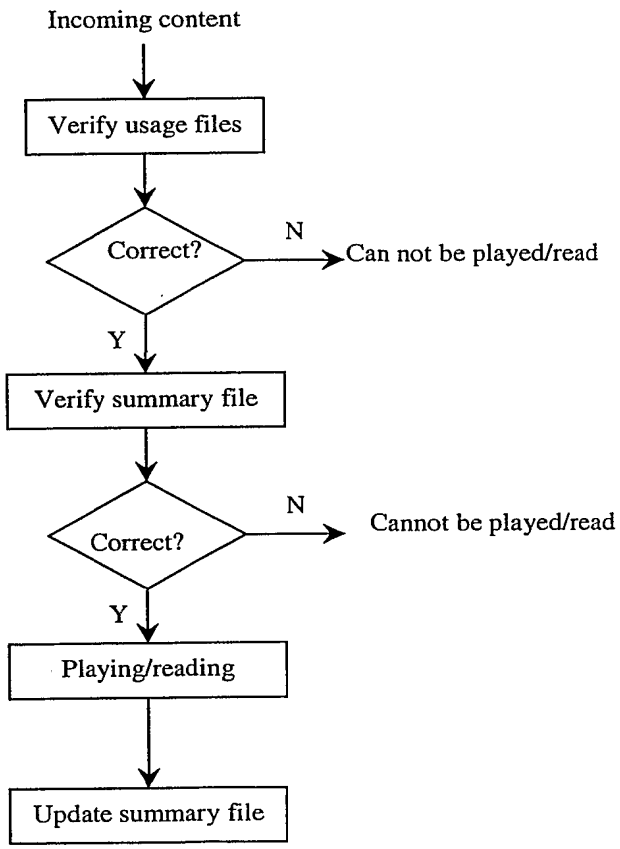

Incoming content
Verify usage files
Correct?
N
Can not be played/read
Y
Verify summary file
Correct?
N
Cannot be played/read
Y
Playing/reading
Update summary file

Fig.7